

IN THE CLAIMS

Please substitute the following amended claims as follows:

1. (Amended) A system comprising:
 - a non-volatile data storage device, configured as one or more storage regions, to store one or more bytes of data;
 - a program store communicatively coupled to the data storage device, the program store to store one or more processor-readable instructions to ascertain the validity of data stored in the non-volatile storage device and if invalid to replace the data with an earlier stored valid image of the data; and
 - a processing unit coupled to the storage device and program store, to read and process the one or more instructions in the program store.
2. (Amended) The system of claim 1 wherein the processing unit is configured to process the instructions in the program store as part of a start-up procedure.
3. (Amended) The system of claim 1 wherein the data stored in the non-volatile data store is a Basic Input Output System (BIOS) for a processing device.
4. The system of claim 1 wherein the processor-readable instructions in the program store ascertain the validity of the data stored in the non-volatile storage device on a region by region basis.
5. The system of claim 1 wherein the earlier stored valid image of the data is stored in a location that cannot be modified without system authorization.
6. The system of claim 5 wherein system authorization includes

2 employing a system interface to perform modifications to the data stored in the
3 non-volatile data storage device.

1 7. The system of claim 1 wherein ascertaining the validity of the data stored in the
2 non-volatile storage device includes

3 determining if the current data in the non-volatile storage device is different than
4 the earlier stored valid image of the data.

1 8. The system of claim 1 wherein ascertaining the validity of the data stored in the
2 non-volatile storage device includes

3 determining if an integrity metric corresponding to the current data in the non-
4 volatile storage device is different than the same integrity metric corresponding to the
5 earlier stored valid image of the data.

1 9. The system of claim 1 further comprising:

2 generating a copy the current data in the non-volatile storage device if an
3 authorized application modifies the current data; and
4 storing the copy as a valid image of the current data.

1 10. (Amended) A method comprising:

2 reading current content stored in a non-volatile storage device;
3 determining if the current content has been modified without authorization; and
4 replacing the current content with a previously stored valid image of the content if
5 the current content is determined to have been modified without authorization.

1 11. (Amended) The method of claim 10 further comprising:

2 reading the valid image of the previously stored content; and
3 comparing the previously stored content to the current content to determine if the
4 current content has been modified.

- 1 12. The method of claim 10 wherein determining if the current content has been
2 modified without authorization includes
3 comparing a previously stored checksum, corresponding to the valid image of the
4 previously stored content, and the checksum corresponding to the current content.
- 1 13. The method of claim 10 wherein determining if the current content has been
2 modified without authorization includes
3 comparing a previously stored cyclic redundancy check value, corresponding to
4 the valid image of the previously stored content, and the cyclic redundancy check value
5 corresponding to the current content.
- 1 14. The method of claim 10 wherein determining if the current content has been
2 modified without authorization includes
3 comparing a previously stored bit mask, corresponding to the valid image of
4 previously stored content, and the corresponding bits of the current content.
- 1 15. The method of claim 10 further comprising:
2 storing a valid image of the current content for later use.
- 1 16. The method of claim 10 wherein the content is read from the non-volatile storage
2 device as part of a start-up procedure.
- 1 17. (Amended) A method comprising:
2 arranging a non-volatile storage device into one or more storage regions;
3 generating an integrity metric corresponding to the valid content stored in a first
4 region of the non-volatile storage device; and
5 storing the integrity metric to later determine if the content in the first region has
6 been modified without authorization.
- 1 18. The method of claim 17 further comprising:

2 comparing a previously stored integrity metric, corresponding to an earlier
3 version of the content stored in the first region, to a newly calculated integrity metric
4 corresponding to the current content stored in the first region to determine if an
5 unauthorized modification has occurred.

1 19. The method of claim 17 further comprising:
2 replacing the first region with an earlier version of the content therein if it is
3 determined that there was an unauthorized modification.

1 20. (Amended) A method comprising:
2 arranging a non-volatile storage device into one or more storage regions; and
3 comparing current content in a first region to an earlier stored image of the
4 content in the first region; and
5 replacing the current content stored in the first region with the previously stored
6 content of the first region if it is determined that there was an unauthorized modification
7 of the current content.

1 21. The method of claim 20 wherein the method is implemented as part of a start-up
2 procedure.

1 22. The method of claim 20 wherein the non-volatile device is arranged into one or
2 more logical regions, each region of one or more bytes.

1 23. A method comprising:
2 arranging a non-volatile storage device into one or more storage regions;
3 verifying that the content in the non-volatile storage device is valid; and
4 encrypting the content in a first region by use a first encryption key to protect it
5 from unauthorized access.

1 24. The method of claim 23 further comprising:
2 protecting the content of the first region from unauthorized modification by use of
3 an integrity metric.

1 25. The method of claim 23 further comprising:
2 protecting the content of the content of a second region with a second encryption
3 key.

1 26. (Amended) A machine-readable medium having one or more instructions for
2 protecting content in a non-volatile storage device against unauthorized use, which
3 when executed by a processor, causes the processor to perform operations comprising:
4 reading current content stored in a non-volatile storage device;
5 determining if the current content has been modified without authorization; and
6 replacing the current content with a previously stored image of the content if the
7 current content is determined to have been modified without authorization.

1 27. The machine-readable medium of claim 26 wherein determining if the current
2 content has been modified without authorization includes
3 reading an image of previously stored content; and
4 comparing the previously stored content to the current content to determine if the
5 current content has been modified.

1 28. The machine-readable medium of claim 26 wherein determining if the current
2 content has been modified without authorization includes
3 comparing a previously stored checksum corresponding to a valid image of
4 previously stored content and the checksum corresponding to the current content.

1 29. The machine-readable medium of claim 26 wherein determining if the current
2 content has been modified without authorization includes
3 comparing a previously stored cyclic redundancy check value corresponding to a
4 valid image of previously stored content and the cyclic redundancy check value
5 corresponding to the current content.

1 30. The machine-readable medium of claim 26 wherein determining if the current
2 content has been modified without authorization includes
123202P16510

3
4

comparing a previously stored bit mask corresponding to a valid image of
previously stored content and the corresponding bits of the current content.
